

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | |
|--------------------------------------|---|-----------------------------|
| In re Application of |) | Group Art Unit: 2435 |
| |) | |
| Xin Xue |) | Examiner: To, Baotran N. |
| |) | |
| Serial No. 10/666,889 |) | |
| |) | APPEAL BRIEF |
| Filed: September 17, 2003 |) | |
| |) | |
| For: METHOD OF AND SYSTEM FOR |) | 162 North Wolfe Road |
| AUTHENTICATION |) | Sunnyvale, California 94086 |
| DOWNLOADING |) | (408) 530-9700 |
| |) | |
| |) | Customer No. 28960 |

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In furtherance of the Applicants' Notice of Appeal filed on January 4, 2010, this Appeal Brief is submitted. This Appeal Brief is submitted in support of the Applicants' Notice of Appeal, and further pursuant to the rejection mailed on October 1, 2009, in which Claims 1-44 were rejected. The Applicants submit this Appeal Brief to the Board of Patent Appeals and Interferences in compliance with the requirements of 37 C.F.R. § 41.37, as stated in *Rules of Practice Before the Board of Patent Appeals and Interferences (Final Rule)*, 69 Fed. Reg. 49959 (August 12, 2004). The Applicants contend that the rejections of Claims 1-44 in this proceeding are in error, were previously overcome and are overcome again by this appeal.

I. REAL PARTIES IN INTEREST

As the assignee of the entire right, title, and interest in the above-captioned patent application, the real parties in interest in this appeal, is:

Sony Corporation, a Japanese corporation
6-7-35 Kitashinagawa, Shinagawa
Tokyo, 141
Japan

Sony Electronics Inc., a corporation of the State of Delaware
1 Sony Drive
Park Ridge, NJ 07656-8003

per the assignment document filed on September 17, 2003.

II. RELATED APPEALS AND INTERFERENCES

The Applicants are not aware of any other appeals or interferences related to the present application.

III. STATUS OF THE CLAIMS

Claims 1-44 are involved in the appeal. Claims 1-44 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication No. 2004/0103064 to Howard et al. ("Howard", a copy of which is attached as Exhibit A) in view of U.S. Patent Application No. 2004/0010467 A1 to Hori et al. ("Hori", a copy of which is attached as Exhibit B).

IV. STATUS OF THE AMENDMENTS FILED AFTER FINAL REJECTION

No amendments have been filed after the Office Action mailed on October 1, 2009.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The invention disclosed in the present application number 10/666,889 is directed to methods, systems and devices for authorization and authentication downloading utilizing a removable memory having a set of authentication data. A user accesses a server with a handheld electronic device via a wireless Internet connection. The removable memory includes the set of authentication data. The handheld electronic device includes an interface to connect to the Internet when the removable memory is inserted into the handheld electronic device and a connection is formed with a server, using the set of authentication data, the server is able to authenticate the removable memory automatically without the user interfacing personally with the server. The server authenticates downloading to the removable memory in the handheld electronic device by reading the set of authentication data on the removable memory, and downloading the desired content to the removable memory.

The elements of Claim 1, directed to one embodiment of the present invention, are described in the Specification at page 6, line 4 through page 7, line 31 and the accompanying figure 4. The method of downloading content from a server 150 to an electronic device 110 comprises storing authentication data on a removable memory 120, wherein the authentication data includes a predetermined level of content access, accessing the server 150 with the electronic device 110, authenticating the removable memory 120 by reading the authentication data from the removable memory 120 to determine the predetermined level of content access and downloading the content from the server 150 to the removable memory 120 according to the predetermined level of content access.

The elements of Claim 10, directed to one embodiment of the present invention, are described in the Specification at page 3, line 15 through page 6, line 3 and the accompanying figures 1-3. The system 100, 135, 145 for downloading content from a server 150 to an electronic device 110 comprises means for storing authentication data on a removable memory 120, wherein the authentication data includes a predetermined level of content access, further wherein the authentication data is preinstalled on the removable memory 120, means for receiving the removable memory 120 in the electronic device 110, means for accessing the server 150 with the electronic device 110, means for authenticating the removable memory 120 by reading the authentication data from the removable memory 120 to determine the predetermined level of content access and means for downloading the content from the server 150 to the removable memory 120 according to the predetermined level of content access.

Means for storing authentication data on a removable memory 120 is shown in Figures 1-3. The electronic device 110 of the authentication system 100 receives the removable memory 120 in a memory slot 130. A set of authentication data is stored electronically on the removable memory 120, and when the removable memory 120 is inserted into the memory slot 130, the set of authentication data is available to authenticate the removable memory 120 to download content from a server 150 (figure 2), wherein the server 150 (figure 2) is accessed by utilizing the wireless capabilities 160 of the electronic device 110 or through a wired connection to the Internet 170 (figure 2). [Present Specification, page 3, line 32 through page 4, line 5]

Means for receiving the removable memory 120 in the electronic device 110 is shown in Figures 1-3. The electronic device 110 of the authentication system 100 receives the removable memory 120 in a memory slot 130. A set of authentication data is stored electronically on the removable memory 120, and when the removable memory 120 is inserted into the memory slot 130, the set of authentication data is available to authenticate the removable memory 120 to download content from a server 150 (figure 2), wherein the server 150 (figure 2) is accessed by utilizing the wireless capabilities 160 of the electronic device 110 or through a wired connection to the Internet 170 (figure 2). [Present Specification, page 3, line 32 through page 4, line 5]

Means for accessing the server 150 with the electronic device is shown in Figures 1-3. While a PDA is depicted here in this embodiment, alternative embodiments utilize other electronic devices 110 capable of housing the removable memory 120 and accessing a server 150 through the Internet using either a wired or wireless connection, including but not limited to, cable, DSL and satellite. [Present Specification, page 3, lines 19-22] The electronic device 110 of the authentication system 100 receives the removable memory 120 in a memory slot 130. A set of authentication data is stored electronically on the removable memory 120, and when the removable memory 120 is inserted into the memory slot 130, the set of authentication data is available to authenticate the removable memory 120 to download content from a server 150 (figure 2), wherein the server 150 (figure 2) is accessed by utilizing the wireless capabilities 160 of the electronic device 110 or through a wired connection to the Internet 170 (figure 2). [Present Specification, page 3, line 32 through page 4, line 5]

Means for authenticating the removable memory 120 is shown in Figures 1-3. The electronic device 110 of the authentication system 100 receives the removable memory 120 in a

memory slot 130. A set of authentication data is stored electronically on the removable memory 120, and when the removable memory 120 is inserted into the memory slot 130, the set of authentication data is available to authenticate the removable memory 120 to download content from a server 150 (figure 2), wherein the server 150 (figure 2) is accessed by utilizing the wireless capabilities 160 of the electronic device 110 or through a wired connection to the Internet 170 (figure 2). [Present Specification, page 3, line 32 through page 4, line 5]

Means for downloading the content from the server 150 to the removable memory 120 is shown in Figures 1-3. While a PDA is depicted here in this embodiment, alternative embodiments utilize other electronic devices 110 capable of housing the removable memory 120 and accessing a server 150 through the Internet using either a wired or wireless connection, including but not limited to, cable, DSL and satellite. [Present Specification, page 3, lines 19-22] The electronic device 110 of the authentication system 100 receives the removable memory 120 in a memory slot 130. A set of authentication data is stored electronically on the removable memory 120, and when the removable memory 120 is inserted into the memory slot 130, the set of authentication data is available to authenticate the removable memory 120 to download content from a server 150 (figure 2), wherein the server 150 (figure 2) is accessed by utilizing the wireless capabilities 160 of the electronic device 110 or through a wired connection to the Internet 170 (figure 2). [Present Specification, page 3, line 32 through page 4, line 5]

The elements of Claim 19, directed to one embodiment of the present invention, are described in the Specification at page 3, line 15 through page 6, line 3 and the accompanying figures 1-3. The system 100, 135, 145 for downloading content comprises a removable memory 120, the removable memory 120 including authentication data, the authentication data including a predetermined level of content access, an electronic device 110 configured to receive the removable memory 120 and a server 150, wherein when the electronic device 110 accesses the server 150, the removable memory 120 is authenticated by reading the authentication data from the removable memory 120 and determining the predetermined level of content access, and further wherein once authenticated, content according to the predetermined level of content access is downloaded from the server 150 to the removable memory 120.

The elements of Claim 28, directed to one embodiment of the present invention, are described in the Specification at page 3, line 15 through page 6, line 3 and the accompanying figures 1-3. The electronic device 110 for downloading comprises a memory slot 130 configured

to receive a removable memory 120, wherein the removable memory 120 includes authentication data, the authentication data including a predetermined level of content access and a communications interface configured for coupling to a server 150, wherein when the electronic device 110 accesses the server 150 through the communications interface, the removable memory 120 is authenticated by reading the authentication data from the removable memory 120 to determine the predetermined level of content access, further wherein content according to the predetermined level of content access is downloaded to the removable memory 120.

The elements of Claim 36, directed to one embodiment of the present invention, are described in the Specification at page 3, line 15 through page 6, line 3 and the accompanying figures 1-3. The removable memory 120 for downloading comprises authentication data, the authentication data including a predetermined level of content access and a communications interface configured for coupling to a server 150, wherein when an electronic device 110 accesses the server 150 through the communications interface, the removable memory 120 is authenticated by reading the authentication data from the removable memory 120 to determine the predetermined level of content access, further wherein the electronic device 110 includes a memory slot 130 configured to receive the removable memory 120, and further wherein content according to the predetermined level of content access is downloaded to the removable memory 120, further wherein the predetermined level of content access determines how much of the content on the server 150 is available for download.

The elements of Claim 44, directed to one embodiment of the present invention, are described in the Specification at page 6, line 4 through page 7, line 31 and the accompanying figure 4. The method of downloading content from a server 150 to an electronic device 110 comprises storing authentication data on a removable memory 120, wherein the authentication data includes a predetermined level of content access, accessing the server 150 with the electronic device 110, authenticating the removable memory 120 by reading the authentication data from the removable memory 120 to determine the predetermined level of content access and automatically downloading the content from the server 150 to the removable memory 120 according to the predetermined level of content access, wherein the authentication data is time stamped, such that the predetermined level of content access is available for a predetermined amount of time.

VI. GROUND OF REJECTION AND OTHER MATTERS TO BE REVIEWED ON APPEAL

The following issues are presented in this Appeal Brief for review by the Board of Patent Appeals and Interferences:

1. Whether Claims 1-44 are properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Howard in view of Hori.

VII. ARGUMENT

Grounds for Rejection

Within the Office Action, Claims 1-44 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Howard in view of Hori.

Outline of Arguments

In the discussion that follows, the Applicants discuss the teachings of Howard and Hori. As will be discussed in detail below, neither Howard nor Hori individually teach the presently claimed invention. Further, the combination of Howard and Hori is improper because there is no motivation to combine the downloading of content from a server to a removable memory of Hori with the model relating to the payment for online content of Howard. Moreover, the combination of Howard and Hori is also improper because it would change Howard's principle mode of operation.

1. Howard does not teach transferring content from a content server to a removable memory.

Howard is directed to a model relating to the payment for online content. Specifically, Howard teaches access is automatically granted to online content when the smart card is inserted into a reader attached to the user's PC, and cut off when the smart card is removed from the reader. [Howard, Abstract] However, as recognized within the Office Action dated February 18, 2009, Howard does not teach content being downloaded from a server to a removable memory. [Office Action of February 18, 2009, pages 7 and 8] Instead, Howard merely discloses transferring content from a content server to a user PC. [Howard, Paragraph 0025] Accordingly, Howard does not teach the presently claimed invention.

2. Hori does not teach the presently claimed invention.

Hori is directed to a memory card that includes a memory to store encrypted content data. [Hori, Abstract] Specifically, Hori teaches a memory card receives the encrypted content data and license through cellular phone 100 and applies decryption on the above encryption, and then provides the decrypted data to the music reproduction unit in the cellular phone. [Hori, 0065] Hori is only cited for the purpose of teaching content being downloaded from a server to a removable memory. Accordingly, Hori does not teach the presently claimed invention.

3. The combination of Howard and Hori is improper because there is no motivation to combine the downloading of content from a server to a removable memory of Hori with the model relating to the payment for online content of Howard.

Within the Office Action of October 1, 2009, it is asserted that the motivation to combine the “downloading of content from a server to removable memory” of Hori with the “model relating to the payment for online content” of Howard would be to prevent distributed copyrighted data from being replicated without permission of the copyright owner. Applicant respectfully disagrees because the asserted motivation would not be accomplished by the proposed combination.

The alleged motivation is nonexistent because there is no indication in Hori that downloading the content to the removable memory instead of the user PC would, on its own, prevent distributed copyrighted data from being replicated without permission of the copyright owner in Howard. On the contrary, Hori’s prevention of impermissible replication relies on the entirety of the invention of Hori, including a complex data storage structure that comprises a plurality of authentication data hold means, a select means, a key hold means, a first decryption means, a session key generation means, a session key encryption means, and a session key decryption means. In other words, even if Howard downloaded the content to the removable memory instead of the PC (as taught by Hori), Howard would be no more protected from copyright violations. Both methods of storage are equally susceptible to copyright infringement. As a result, Howard would not be motivated to incorporate Hori for the above asserted

motivation because it would not provide any benefit (i.e. no increased copyright protection) while instead increasing complexity. An inventor would not be motivated to combine two prior art references in order to achieve copyright protection benefits, if the asserted combination would not actually result in those benefits. Accordingly, the combination of Howard and Hori is improper because there is no motivation for their combination.

4. The combination of Howard and Hori is improper because it would change Howard's principle mode of operation.

The MPEP states “[i]f the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. In re Ratti, 270 F.2d 810, 123 (CCPA 1959); MPEP §2143.01. Here, the invention of Howard operates under the principle that the content is downloaded to the user PC, not the removable memory. [Howard, paragraph 0025] As a result, modifying the invention of Howard to download the content to the removable memory instead of the user PC as in Hori is impermissible because it would change its principle mode of operation. Moreover, this impermissibility of the combination is even more apparent if all the elements necessary to actually achieve copyright protection Hori were used to modify Howard. Specifically, such a modification of Howard would only further significantly, unnecessarily, and undesirably complicate Howard while simultaneously changing Howard's principle mode of operation. The extent to which Howard would need to be altered in order to incorporate the whole copyright protection means of Hori, as described above, would certainly result in a change to Howard's principal mode of operation because it would change the components and operation of both Howard's smart card and smart card reader. Accordingly, the combination of Howard and Hori is improper because it changes Howard's principle mode of operation.

5. The claims distinguish over Howard, Hori and their combination.

The claims are grouped separately below to indicate that they do not stand or fall together.

a. Claims 1-9

The independent Claim 1 is directed to a method of downloading content from a server to an electronic device. The method of Claim 1 comprises storing authentication data on a removable memory, wherein the authentication data includes a predetermined level of content access, accessing the server with the electronic device, authenticating the removable memory by reading the authentication data from the removable memory to determine the predetermined level of content access and downloading the content from the server to the removable memory according to the predetermined level of content access. As described above, the combination of Howard and Hori is improper. For at least these reasons, the independent Claim 1 is allowable over the teachings of Howard, Hori and their combination.

Claims 2-9 are dependent on the independent Claim 1. As described above, the independent Claim 1 is allowable over the teachings of Howard, Hori and their combination. Accordingly, Claims 2-9 are all also allowable as being dependent on an allowable base claim.

b. Claims 10-18

The independent Claim 10 is directed to a system for downloading content from a server to an electronic device. The system of Claim 10 comprises means for storing authentication data on a removable memory, wherein the authentication data includes a predetermined level of content access, further wherein the authentication data is preinstalled on the removable memory, means for receiving the removable memory in the electronic device, means for accessing the server with the electronic device, means for authenticating the removable memory by reading the authentication data from the removable memory to determine the predetermined level of content access and means for downloading the content from the server to the removable memory according to the predetermined level of content access. As described above, the combination of Howard and Hori is improper. For at least these reasons, the independent Claim 10 is allowable over the teachings of Howard, Hori and their combination.

Claims 11-18 are dependent on the independent Claim 10. As described above, the independent Claim 10 is allowable over the teachings of Howard, Hori and their combination. Accordingly, Claims 11-18 are all also allowable as being dependent on an allowable base claim.

c. Claims 19-27

The independent Claim 19 is directed to a system for downloading content. The system of Claim 19 comprises a removable memory, the removable memory including authentication data, the authentication data including a predetermined level of content access, an electronic device configured to receive the removable memory and a server, wherein when the electronic device accesses the server, the removable memory is authenticated by reading the authentication data from the removable memory and determining the predetermined level of content access, and further wherein once authenticated, content according to the predetermined level of content access is downloaded from the server to the removable memory. As described above, the combination of Howard and Hori is improper. For at least these reasons, the independent Claim 19 is allowable over the teachings of Howard, Hori and their combination.

Claims 20-27 are dependent on the independent Claim 19. As described above, the independent Claim 19 is allowable over the teachings of Howard, Hori and their combination. Accordingly, Claims 20-27 are all also allowable as being dependent on an allowable base claim.

d. Claims 28-35

The independent Claim 28 is directed to an electronic device for downloading. The device of Claim 28 comprises a memory slot configured to receive a removable memory, wherein the removable memory includes authentication data, the authentication data including a predetermined level of content access and a communications interface configured for coupling to a server, wherein when the electronic device accesses the server through the communications interface, the removable memory is authenticated by reading the authentication data from the removable memory to determine the predetermined level of content access, further wherein content according to the predetermined level of content access is downloaded to the removable memory. As described above, the combination of Howard and Hori is improper. For at least these reasons, the independent Claim 28 is allowable over the teachings of Howard, Hori and their combination.

Claims 29-35 are dependent on the independent Claim 28. As described above, the independent Claim 28 is allowable over the teachings of Howard, Hori and their combination. Accordingly, Claims 29-35 are all also allowable as being dependent on an allowable base claim.

e. Claims 36-43

The independent Claim 36 is directed to a removable memory for downloading. The removable memory of Claim 36 comprises authentication data, the authentication data including a predetermined level of content access and a communications interface configured for coupling to a server, wherein when an electronic device accesses the server through the communications interface, the removable memory is authenticated by reading the authentication data from the removable memory to determine the predetermined level of content access, further wherein the electronic device includes a memory slot configured to receive the removable memory, and further wherein content according to the predetermined level of content access is downloaded to the removable memory, further wherein the predetermined level of content access determines how much of the content on the server is available for download. As described above, the combination of Howard and Hori is improper. For at least these reasons, the independent Claim 36 is allowable over the teachings of Howard, Hori and their combination.

Claims 37-43 are dependent on the independent Claim 36. As described above, the independent Claim 36 is allowable over the teachings of Howard, Hori and their combination. Accordingly, Claims 37-43 are all also allowable as being dependent on an allowable base claim.

f. Claim 44

The independent Claim 44 is directed to a method of downloading content from a server to an electronic device. The method of Claim 44 comprises storing authentication data on a removable memory, wherein the authentication data includes a predetermined level of content access, accessing the server with the electronic device, authenticating the removable memory by reading the authentication data from the removable memory to determine the predetermined level of content access and automatically downloading the content from the server to the removable memory according to the predetermined level of content access, wherein the authentication data is time stamped, such that the predetermined level of content access is available for a predetermined amount of time. As described above, the combination of Howard and Hori is improper. For at least these reasons, the independent Claim 44 is allowable over the teachings of Howard, Hori and their combination.

6. CONCLUSION

For the above reasons, it is respectfully submitted that the Claims 1-44 are allowable over the cited prior art references. Therefore, a favorable indication is respectfully requested.

Respectfully submitted,
HAVERSTOCK & OWENS LLP

Dated: February 26, 2010

By: /Jonathan O. Owens/
Jonathan O. Owens
Reg. No.: 37,902
Attorney for Applicant

VIII. CLAIMS APPENDIX

This appendix includes a list of the claims under appeal.

1. A method of downloading content from a server to an electronic device, comprising:
storing authentication data on a removable memory, wherein the authentication data includes a predetermined level of content access;
accessing the server with the electronic device;
authenticating the removable memory by reading the authentication data from the removable memory to determine the predetermined level of content access; and
downloading the content from the server to the removable memory according to the predetermined level of content access.
2. The method according to claim 1 wherein the authenticating is performed by the server.
3. The method according to claim 1 wherein the removable memory is a semiconductor memory.
4. The method according to claim 1 further comprising time stamping the authentication data, such that the predetermined level of content access is available for a predetermined amount of time.
5. The method according to claim 1 wherein the server is accessed through a wired internet connection, further wherein the wired internet connection includes a conduit and a personal computer.
6. The method according to claim 1 wherein the server is accessed through a wireless connection.
7. The method according to claim 6 wherein the wireless connection includes an internet connection.

8. The method according to claim 6 wherein the wireless connection includes a local area network.
9. The method according to claim 6 wherein the wireless connection includes a wide area network.
10. A system for downloading content from a server to an electronic device, comprising:
 - means for storing authentication data on a removable memory, wherein the authentication data includes a predetermined level of content access, further wherein the authentication data is preinstalled on the removable memory;
 - means for receiving the removable memory in the electronic device;
 - means for accessing the server with the electronic device;
 - means for authenticating the removable memory by reading the authentication data from the removable memory to determine the predetermined level of content access; and
 - means for downloading the content from the server to the removable memory according to the predetermined level of content access.
11. The system according to claim 10 wherein the means for authenticating is included within the server.
12. The system according to claim 10 wherein the removable memory is a semiconductor memory.
13. The system according to claim 10 wherein the authentication data also includes a time stamp, such that the predetermined level of content access is available for a predetermined amount of time.
14. The system according to claim 10 wherein the means for accessing accesses the server through a wired internet connection, further wherein the wired internet connection includes a conduit and a personal computer.
15. The system according to claim 10 wherein the means for accessing accesses the server through a wireless connection.

16. The system according to claim 15 wherein the wireless connection includes an internet connection.
17. The system according to claim 15 wherein the wireless connection includes a local area network.
18. The system according to claim 15 wherein the wireless connection includes a wide area network.
19. A system for downloading content, comprising:
a removable memory, the removable memory including authentication data, the authentication data including a predetermined level of content access;
an electronic device configured to receive the removable memory; and
a server, wherein when the electronic device accesses the server, the removable memory is authenticated by reading the authentication data from the removable memory and determining the predetermined level of content access, and further
wherein once authenticated, content according to the predetermined level of content access is downloaded from the server to the removable memory.
20. The system according to claim 19 wherein the server performs the authentication of the removable memory.
21. The system according to claim 19 wherein the removable memory is a semiconductor memory.
22. The system according to claim 19 wherein the authentication data is time stamped, such that the predetermined level of content access is available for a predetermined amount of time.
23. The system according to claim 19 wherein the server is accessed through a wired internet connection, further wherein the wired internet connection includes a conduit and a personal computer.

24. The system according to claim 19 wherein the server is accessed through a wireless connection.
25. The system according to claim 24 wherein the wireless connection includes an internet connection.
26. The system according to claim 24 wherein the wireless connection includes a local area network.
27. The system according to claim 24 wherein the wireless connection includes a wide area network.
28. An electronic device for downloading, comprising:
 - a memory slot configured to receive a removable memory, wherein the removable memory includes authentication data, the authentication data including a predetermined level of content access; and
 - a communications interface configured for coupling to a server, wherein when the electronic device accesses the server through the communications interface, the removable memory is authenticated by reading the authentication data from the removable memory to determine the predetermined level of content access,
 - further wherein content according to the predetermined level of content access is downloaded to the removable memory.
29. The electronic device according to claim 28 wherein the server performs the authentication of the removable memory.
30. The electronic device according to claim 28 wherein the removable memory is a semiconductor memory.
31. The electronic device according to claim 28 wherein the authentication data is time stamped, such that the predetermined level of content access is available for a predetermined amount of time.

32. The electronic device according to claim 28 wherein the communications interface is a wired internet connection, further wherein the wired internet connection includes a conduit and a personal computer.
33. The electronic device according to claim 28 wherein the communications interface is a wireless connection, the wireless connection including an internet connection.
34. The electronic device according to claim 33 wherein the wireless connection includes a local area network.
35. The electronic device according to claim 33 wherein the wireless connection includes a wide area network.
36. A removable memory for downloading, comprising:
authentication data, the authentication data including a predetermined level of content access; and
a communications interface configured for coupling to a server, wherein when an electronic device accesses the server through the communications interface, the removable memory is authenticated by reading the authentication data from the removable memory to determine the predetermined level of content access, further wherein the electronic device includes a memory slot configured to receive the removable memory, and further
wherein content according to the predetermined level of content access is downloaded to the removable memory, further wherein the predetermined level of content access determines how much of the content on the server is available for download.
37. The removable memory according to claim 36 wherein the server performs the authentication of the removable memory.
38. The removable memory according to claim 36 wherein the removable memory is a semiconductor memory.

39. The removable memory according to claim 36 wherein the authentication data is time stamped, such that the predetermined level of content access is available for a predetermined amount of time.
40. The removable memory according to claim 36 wherein the communications interface is a wired internet connection, further wherein the wired internet connection includes a conduit and a personal computer.
41. The removable memory according to claim 36 wherein the communications interface is a wireless connection, the wireless connection including an internet connection.
42. The removable memory according to claim 41 wherein the wireless connection includes a local area network.
43. The removable memory according to claim 41 wherein the wireless connection includes a wide area network.
44. A method of downloading content from a server to an electronic device, comprising:
storing authentication data on a removable memory, wherein the authentication data includes a predetermined level of content access;
accessing the server with the electronic device;
authenticating the removable memory by reading the authentication data from the removable memory to determine the predetermined level of content access; and
downloading the content from the server to the removable memory according to the predetermined level of content access;
wherein the authentication data is time stamped, such that the predetermined level of content access is available for a predetermined amount of time.

IX. EVIDENCE APPENDIX

STATEMENT

Pursuant to 37 C.F.R. § 41.37(c)(1)(ix), the following is a statement setting forth where in the record the evidence of this appendix was entered by the examiner:

| Evidence Description: | Where Entered: |
|---------------------------------|--|
| U.S. Pat. App. No. 2004/0103064 | Office Action mailed February 18, 2009 |
| U.S. Pat. App. No. 2004/0010467 | Office Action mailed January 29, 2007 |
| Office Action October 1, 2009 | Examiner Office Action |
| Office Action February 18, 2009 | Examiner Office Action |

X. RELATED PROCEEDINGS APPENDIX

There are no related proceedings.